Group = Symmetry

Samuel J. Lomonaco, Jr.
Dept. of Comp. Sci. & Electrical Engineering
University of Maryland Baltimore County
Baltimore, MD 21250
Email: Lomonaco@UMBC.EDU
WebPage: http://www.csee.umbc.edu/~lomonaco
UMBC

Defense Advanced Research Projects Agency (DARPA) &
Air Force Research Laboratory, Air Force Materiel Command, USAF
Agreement Number F30602-01-2-0522

This work is supported by:

- The Defense Advance Research Projects Agency (DARPA) & Air Force Research Laboratory (AFRL), Air Force Materiel Command, USAF Agreement Number F30602-01-2-0522.
- The National Institute for Standards and Technology (NIST)
- The Mathematical Sciences Research Institute (MSRI).
- The Institute for Scientific Interchange
- L-O-O-P The L-O-O-P Fund.

Definition of a Group

This definition took 100s of years to develop !

Why is it so important ?

Purpose

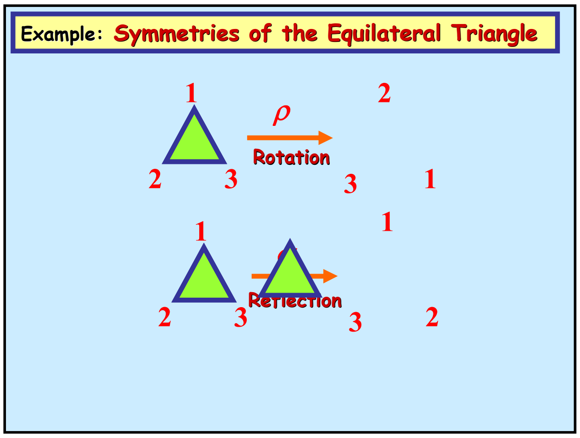
A Group is a Mathematical Tool for Quantifying Symmetry

Definition of a Group

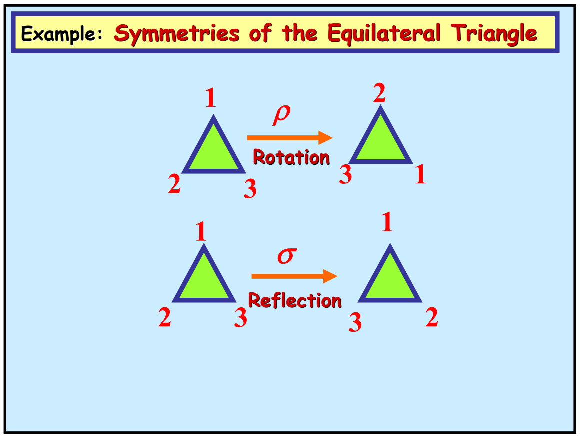
Definition. A group is a set G together with a binary operation $\bullet : G \times G \rightarrow G$ satisfying the following axioms:

- $g_1 \bullet (g_2 \bullet g_3) = (g_1 \bullet g_2) \bullet g_3, \quad \forall g_1, g_2, g_3 \in G$
- There exists a unique element 1, called the identity, such that $1 \bullet g = g = g \bullet 1, \quad \forall g \in G$
- $\forall g \in G$, there exists a unique element g^{-1}, called the inverse of g, such that

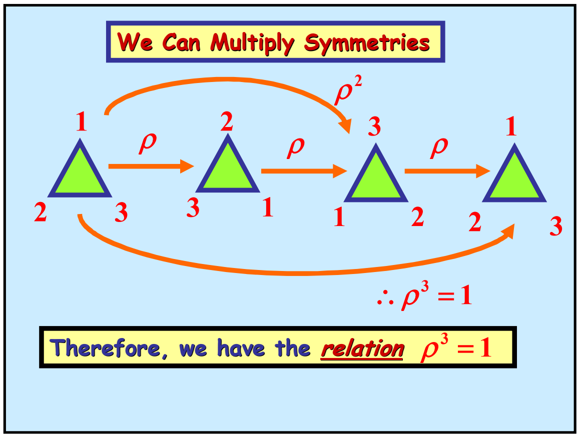
$$g \bullet g^{-1} = 1 = g^{-1} \bullet g$$



Example: *Symmetries of the Equilateral Triangle*



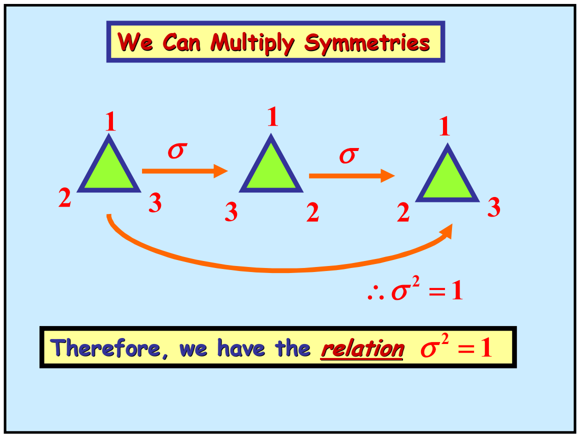
Example: *Symmetries of the Equilateral Triangle*



We Can Multiply Symmetries

$\therefore \rho^3 = 1$

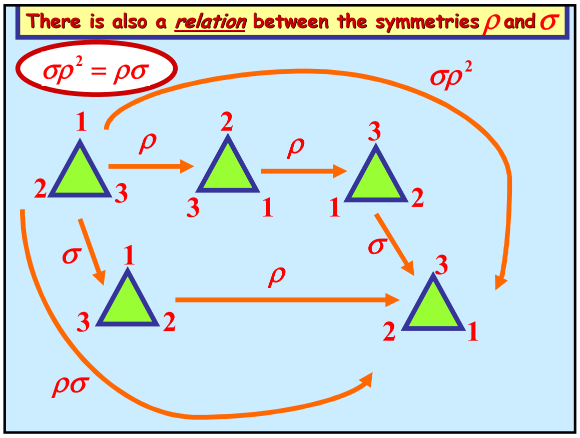
Therefore, we have the ***relation*** $\rho^3 = 1$



We Can Multiply Symmetries

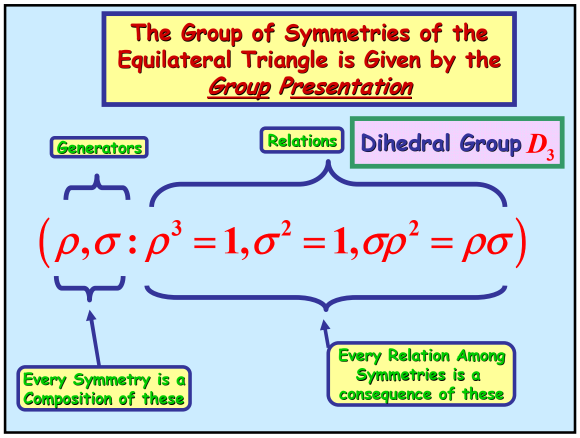
$\therefore \sigma^2 = 1$

Therefore, we have the ***relation*** $\sigma^2 = 1$



There is also a *relation* between the symmetries ρ and σ

$\sigma\rho^2 = \rho\sigma$

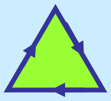


The Group of Symmetries of the Equilateral Triangle is Given by the ***Group Presentation***

Dihedral Group D_3

$$\left(\overbrace{\underbrace{\rho,\sigma}_{\text{Every Symmetry is a Composition of these}}}^{\text{Generators}}:\overbrace{\underbrace{\rho^3=1,\sigma^2=1,\sigma\rho^2=\rho\sigma}_{\text{Every Relation Among Symmetries is a consequence of these}}}^{\text{Relations}}\right)$$

Example: Symmetries of the Oriented Equilateral Triangle



$$\mathbb{Z}_3 = (\rho : \rho^3 = 1)$$

Cyclic Group of Order 3

Example: Symmetries of the Regular n-gon

$$(\rho, \sigma : \rho^n = 1, \sigma^2 = 1, \rho^{n-1}\sigma = \sigma\rho)$$

Dihedral Group D_n

Example: Symmetries of Oriented Regular n-gon

$$(\rho : \rho^n = 1)$$

Cyclic Group of Order n $\mathbb{Z}_n$

More Generally, a ***group presentation*** is of the following form:

$$(\underbrace{x_0, x_1, \ldots, x_{n-1}}_{\text{Generators}} : \underbrace{r_0 = 1, r_1 = 1, r_{m-1} = 1}_{\text{Relations}})$$

Free Groups

A group **F** is free if the only relations among its generators are those required for **F** to be a group

$$F = (x_0, x_1, \ldots, x_{n-1} :)$$

- Allowed: $x_i x_i^{-1} = 1$
- Not Allowed: $x_i x_j = x_j x_i, \quad i \neq j$
- Not Allowed: $x_i^3 = 1$

Free Abelian Groups

A group **A** is free abelian if the only relations among its generators are those required for **A** to be an abelian group

$$A = (x_0, x_1, \ldots, x_{n-1} : x_i x_j = x_j x_i \forall i, j)$$

- Allowed: $x_i x_i^{-1} = 1$
- Allowed: $x_i x_j = x_j x_i, \quad i \neq j$
- Not Allowed: $x_i^3 = 1$


???
QUANTUM
COMPUTING
FOR DOGS